A polynomial time attack on instances of M-SIDH and FESTA

Wouter Castryck and Frederik Vercauteren

firstname.lastname@esat.kuleuven.be

COSIC, KU Leuven, Belgium

Abstract. The recent devastating attacks on SIDH rely on the fact that the protocol reveals the images $\varphi(P)$ and $\varphi(Q)$ of the secret isogeny $\varphi : E_0 \to E$ on a basis $\{P, Q\}$ of the N-torsion subgroup $E_0[N]$ where $N^2 > \deg(\varphi)$. To thwart this attack, two recent proposals, M-SIDH and FESTA, proceed by only revealing the images upto unknown scalars $\lambda_1, \lambda_2 \in \mathbb{Z}_N^\times$, i.e. only $\lambda_1\varphi(P)$ and $\lambda_2\varphi(Q)$ are revealed, where $\lambda_1 = \lambda_2$ for M-SIDH and $\lambda_1 = \lambda_2^{-1}$ for FESTA. Similar information is leaked in CSIDH since φ maps the eigenspaces of Frobenius on E_0 to the corresponding eigenspaces on E.

In this paper, we introduce a new polynomial time attack that generalizes the well known "lollipop" attack and analyze how it applies to M-SIDH, FESTA and CSIDH. We show that M-SIDH can be broken in polynomial time whenever E_0 or E is $\mathbb{F}_p$-rational, even when the endomorphism rings of E_0 and E are unknown. This can be generalized to the case where the starting (or end) curve is not $\mathbb{F}_p$-rational, but is connected to its Frobenius conjugate by an isogeny of small degree.

For FESTA, where the curve E_0 is already $\mathbb{F}_p$-rational, we obtain a polynomial time attack under the added requirement that at least one of the basis points P, Q spans an eigenspace of Frobenius, of an endomorphism of low degree, or of a composition of both. We note that the current implementation of FESTA does not choose such a basis. Since it is always possible to construct an endomorphism, typically of large degree, with either P, Q an eigenvector, we conclude that FESTA with overstretched parameters is insecure.

Although the information leaked in CSIDH is very similar to FESTA, we show that our attack does not reveal any new information about the secret isogeny, i.e. we only learn that it is $\mathbb{F}_p$-rational, which is a priori knowledge.

Finally, we analyze if and how it would be possible to backdoor M-SIDH and FESTA by choosing system parameters that look inconspicuous, but in fact reduce to the special cases above via a secret isogeny chosen by the adversary.

Keywords: Isogeny-based cryptography, Frobenius, M-SIDH, FESTA, CSIDH

* This work was supported in part by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement ISOCRYPT - No. 101020788) and by CyberSecurity Research Flanders with reference number VR20192203. Date of this document: 21st September 2023.

1 Introduction

The Supersingular Isogeny Diffie-Hellman (SIDH) protocol [16] and the corresponding key encapsulation mechanism SIKE [1] were once considered to be the pinnacle of isogeny-based cryptography, due to their efficiency and compactness. A recent series of papers [4, 19, 21] resulted in a practical polynomial time attack, exploiting the extra information about the secret isogeny given out by the SIDH/SIKE protocols. In particular, let $\varphi : E_0 \to E$ be a secret isogeny of known degree d, then SIDH/SIKE also reveals the images $\varphi(P)$ and $\varphi(Q)$ of a basis $\{P, Q\}$ for $E[N]$ where N is a large power of a small prime with $\gcd(N, d) = 1$. Given these images, as long as $N^2 > d$ and d is known, the above attack allows to recover the secret isogeny φ in polynomial time. Since the attack really requires the exact knowledge of $\varphi(P)$ and $\varphi(Q)$, it is natural to look for countermeasures that do not reveal such information. However, building an actual functioning SIDH-like protocol seems to be impossible without revealing at least some partial information.

The first approach in this direction was devised by Fouotsa, Moriya and Petit [15] resulting in two protocols: M-SIDH (Masked torsion points SIDH) and MD-SIDH (Masked Degree SIDH). In M-SIDH the degree of the secret isogeny is known, but the images of the torsion points are scaled by a random secret integer $\lambda \in \mathbb{Z}_N^\times$, i.e. the protocol only reveals $\lambda\varphi(P)$ and $\lambda\varphi(Q)$. In MD-SIDH, not only the images of the points are scaled, but the degree of the secret isogeny is also hidden. As shown by the authors in [15], the MD-SIDH problem reduces to the M-SIDH problem, so in the remainder of the paper we will only deal with M-SIDH. The reason why both scalars have to be the same is that the protocol requires that the subgroup $\langle \alpha\lambda\varphi(P) + \beta\lambda\varphi(Q)\rangle$ for random $\alpha, \beta \in \mathbb{Z}_N^\times$ is exactly the same subgroup as $\langle \alpha\varphi(P) + \beta\varphi(Q)\rangle$.

By bilinearity and compatibility of the Weil pairing e_N with isogenies, we can in fact derive $\lambda^2 \bmod N$ via a single discrete logarithm (which is easy since N is smooth):

$$e_N(\lambda\varphi(P), \lambda\varphi(Q)) = e_N(P, Q)^{\lambda^2 d}.$$

As such we can always reduce to the case where $\lambda^2 = 1 \bmod N$, so for M-SIDH to be s-bit secure we require at least 2^s square roots of unity. This requires N to have at least s small distinct prime factors, and as shown in [15] one really requires $2s$ factors. Furthermore, since the N_A used by Alice needs to be coprime with the N_B used by Bob, we end up with a prime p such that $p+1$ is divisible by at least $4s$ small distinct primes. In particular, even for 128-bit security, the prime p is close to 6000 bits, which makes M-SIDH much slower than SIDH.

The second such approach is called FESTA [3] by Basso, Maino and Pope. Here the authors reveal $\lambda_1\varphi(P)$ and $\lambda_2\varphi(Q)$ where λ_1 can be different from λ_2.[1] However, as explained above, this blocks a straightforward adaptation of the

[1] We note that the authors consider a slightly more general setting where

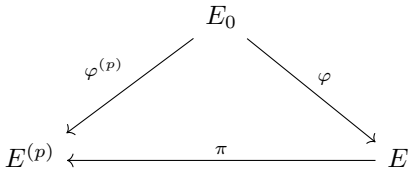
$$\mathbf{A} \cdot \begin{pmatrix} \varphi(P) \\ \varphi(Q) \end{pmatrix}$$

SIDH protocol. To circumvent this problem, the authors construct a trapdoor one-way function, where knowledge of the secret λ_i allows to invert the one-way function. Furthemore, using the same Weil paring trick as above we can derive $\lambda_1\lambda_2 \bmod N$, so we can always reduce to the case where $\lambda_2 = \lambda_1^{-1} \bmod N$.

Although CSIDH [6] does not explicitly reveal torsion point information, there is an implicit leak: since the isogenies used in CSIDH are $\mathbb{F}_p$-rational, we have $\varphi \circ \pi_0 = \pi \circ \varphi$, where π_0, π denote the Frobenius endomorphisms on E_0 and E. Since the characteristic polynomial of these Frobenius endomorphisms is given by $x^2 + p$, we conclude that for N a power of an odd prime ℓ with $\left(\frac{-p}{\ell}\right) = 1$, they will have two different eigenvalues modulo N, say $\mu_1 \neq \mu_2 \bmod N$. Note that using the Chinese Remainder Theorem we are not limited to N being powers of a small prime, but we can deal with any odd N as long as for each prime factor ℓ_i of N we have $\left(\frac{-p}{\ell_i}\right) = 1$. Now assume $P \in E_0[N]$ is an eigenvector with eigenvalue μ_1, i.e. $\pi_0(P) = \mu_1 P$, then applying φ to both sides and using commutativity with Frobenius shows that $\pi(\varphi(P)) = \mu_1\varphi(P)$, so $\varphi(P)$ lies in the μ_1-eigenspace of π on $E[N]$. Therefore if $S \in E[N]$ is an eigenvector of π on $E[N]$ with eigenvalue μ_1, we know there exists some λ_1 such that $S = \lambda_1\varphi(P)$ (and similarly for the other eigenspace). As such, at first glance, the CSIDH case looks very similar to the FESTA case.

The main security argument for both M-SIDH and FESTA is that the polynomial time attack on SIDH no longer applies since the exact images of the torsion points are not revealed and thus it is impossible to recover $\varphi : E_0 \to E$. Although this reasoning is correct when one focuses on the isogeny φ itself, it does not rule out other polynomial time attacks when considering a different, but related isogeny, in particular an isogeny that does not map from E_0 to E. The main idea underlying our attack (which is a generalization of the "lollipop attack" from [15, §4.2-4.3]) is as follows: since we do not know the exact images of the torsion points due to the presence of the λ_i, we will construct a new isogeny ψ (related to φ) from E to some other curve E' that is oblivious to the unknown λ_i.

To illustrate this idea, assume we are attacking M-SIDH where E_0 is $\mathbb{F}_p$-rational. Then consider the following diagram:



Here $E^{(p)}$ denotes the Frobenius conjugate of E, i.e. the curve obtained by raising all coefficients of E to the p-th power, and $\pi : E \to E^{(p)}$ the connecting Frobenius isogeny. The isogeny $\varphi^{(p)}$ is the Frobenius conjugate of φ and satisfies

is revealed, with $\mathbf{A}$ sampled from a commutative subgroup $X \subseteq \mathrm{GL}_2(\mathbb{Z}_N)$. However, as also stated by the authors, there seems little advantage over using diagonal matrices.

$\varphi^{(p)} \circ \pi_0 = \pi \circ \varphi$ with π_0 the Frobenius endomorphism on E_0 (recall that E_0 is assumed to be $\mathbb{F}_p$-rational).

Consider now the isogeny $\psi = \varphi^{(p)} \circ \hat{\varphi}$ from E to $E^{(p)}$ of degree d^2. Denote with $T = \lambda\varphi(P)$ and $S = \lambda\varphi(Q)$ the points revealed by the M-SIDH protocol, then an easy calculation (see Lemma 3) shows that in this case

$$\psi \begin{pmatrix} S \\ T \end{pmatrix} = d \cdot \mathbf{M}_{\pi_0}^{-1} \cdot \pi \begin{pmatrix} S \\ T \end{pmatrix}, \tag{1}$$

where $\mathbf{M}_{\pi_0}$ is such that

$$\pi_0 \begin{pmatrix} P \\ Q \end{pmatrix} = \mathbf{M}_{\pi_0} \begin{pmatrix} P \\ Q \end{pmatrix},$$

i.e., it is the transpose of the matrix of π_0 acting on $E_0[N]$ with respect to the basis $\{P, Q\}$. Since all quantities in equation (1) are known, we can compute the exact images of S, T under ψ and thus the polynomial time attack on SIDH (see Theorem 1) can be applied to recover ψ since in M-SIDH we have $N > d$ and thus $N^2 > \deg(\psi) = d^2$. If ψ is cyclic, we can recover the kernel of $\hat{\varphi}$ since in this case $\ker(\hat{\varphi}) = \ker(\psi)[d]$. Even if ψ is not fully cyclic, it typically remains possible to derive almost all information about φ; see Section 3.2.

A similar attack applies to FESTA with the main difference being that (1) is generalized to

$$\psi \begin{pmatrix} S \\ T \end{pmatrix} = d \cdot \mathbf{D} \cdot \mathbf{M}_{\pi_0}^{-1} \cdot \mathbf{D}^{-1} \cdot \pi \begin{pmatrix} S \\ T \end{pmatrix}, \tag{2}$$

with $\mathbf{D}$ the diagonal matrix with λ_1, λ_2 as entries. Since now $\lambda_1 \neq \lambda_2$ we are faced with the problem that in general the matrix product $\mathbf{D} \cdot \mathbf{M}_{\pi_0}^{-1} \cdot \mathbf{D}^{-1}$ does not simplify to $\mathbf{M}_{\pi_0}^{-1}$ unless $\mathbf{M}_{\pi_0}$ itself is a diagonal matrix; or to put it differently, P, Q need to be eigenvectors of π_0.

Since the information revealed in CSIDH is similar to FESTA, we arrive at the same equation (2) above, where P, Q are now indeed eigenvectors of Frobenius, so we will be able to recover the isogeny $\psi = \varphi^{(p)} \circ \hat{\varphi}$ (assuming we know the degree d of φ which is required in (2) but also in the polynomial time attack on SIDH). However, since φ is $\mathbb{F}_p$-rational by construction, we have that $\varphi^{(p)} = \varphi$ and we simply recover the isogeny $\psi = \varphi \circ \hat{\varphi} = [d]$, so the attack reveals no new information.

Contributions

- We formalize the above attack strategy resulting in a polynomial time attack on the M-SIDH protocol when E_0 is $\mathbb{F}_p$-rational and similarly on the FESTA protocol when E_0 is $\mathbb{F}_p$-rational, but with the added constraint that at least one of P or Q is an eigenvector of π_0. Of course, by focusing on $\hat{\varphi} : E \to E_0$ rather than on φ, the same conclusions apply in case E is $\mathbb{F}_p$-rational.
- We generalize this attack (see Figure 1 for a pictorial representation) to cases where E_0 is not $\mathbb{F}_p$-rational and where we allow for different maps

than Frobenius. Furthermore, we also deal with the more general case of non-diagonal matrices, where we are given

$$\begin{pmatrix} S \\ T \end{pmatrix} = \mathbf{A} \begin{pmatrix} \varphi(P) \\ \varphi(Q) \end{pmatrix}$$

with $\mathbf{A}$ sampled from some public set $X \subseteq \mathrm{GL}_2(\mathbb{Z}_N)$. This generalized attack encompasses known constructions such as the "lollipop endomorphism" from [14] and the corresponding polynomial time attacks on M-SIDH from [15, §4.2-4.3]. Furthermore, we show that this generalized attack results in many more weak bases for FESTA than just eigenspaces of Frobenius (but still a negligible number, so the probability of hitting such bases via random sampling is low) and that it also applies to FESTA with overstretched parameters, i.e. where the order N is artificially larger than what is used in FESTA.

– We analyze the impact of our attack on CSIDH and conclude that there is no impact, i.e. the only information we learn from the attack is a priori knowledge.
– We discuss the possibilities for an attacker to backdoor systems such as M-SIDH and FESTA by using a secret isogeny that reduces the system parameters to the weak instances above and analyze if and how such a backdoor can be detected.

Acknowledgments We thank the anonymous reviewers and the shepherd for the many suggestions for improving our exposition. We also thank Boris Fouotsa, Chenfeng He, Péter Kutas, Guido Lido, Simon-Philipp Merz, Christophe Petit Antonio Sanso and Benjamin Wesolowski for helpful discussions.

2 Background

We assume some basic familiarity with elliptic curves and isogenies; for a self-contained overview we refer the reader to the excellent notes of De Feo [12].

We briefly recall how the different protocols such as SIDH [16], M-SIDH [15], FESTA [3] and CSIDH [6] reveal partial information about a secret isogeny $\varphi : E_0 \to E$. We refer to the corresponding papers for the full protocols; here we focus only on which partial information is revealed and how the degree of the secret isogeny relates to the order of the points on which said partial information is leaked.

These protocols work with supersingular elliptic curves over $\mathbb{F}_p$, in the case of CSIDH, or over $\mathbb{F}_{p^2}$, for the other protocols. An elliptic curve $E/\mathbb{F}_q$ with $q = p^n$ is called supersingular if its trace of Frobenius $t = q + 1 - \#E(\mathbb{F}_q)$ satisfies $p \mid t$. In the cryptographic setting, p is a large prime, so for a supersingular elliptic curve E over $\mathbb{F}_p$ we have $\#E(\mathbb{F}_p) = p + 1$ since $|t| \leq 2\sqrt{q}$, and consequently $\#E(\mathbb{F}_{p^2}) = (p+1)^2$. The protocols that work with supersingular curves E over $\mathbb{F}_{p^2}$ all start an isogeny walk from a curve over $\mathbb{F}_p$ and for such curves we thus

have $\#E(\mathbb{F}_{p^2}) = (p+1)^2$ via Tate's isogeny theorem. Furthermore, their group structure is given by

$$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}\,.$$

To speed-up isogeny computations it is advantageous to work with curves that have many small rational subgroups, and as such the primes used have a specific form $p = fN - 1$ where f is a small co-factor and N is a smooth number. When $N = \ell_1^n \ell_2^m$ for small primes ℓ_i we call p an SIDH-prime; when $N = \prod \ell_i^{e_i}$ for many different small primes ℓ_i and small e_i, we call p a CSIDH-prime.

2.1 SIDH

SIDH [16] is a Diffie-Hellman type key exchange where partial information is revealed to allow the participants in the protocol to complete the following commutatitive diagram:

$$\begin{array}{ccc} E_0, P_A, Q_A, P_B, Q_B & \xrightarrow{\varphi_A} & E_A = E/\langle G_A\rangle, \varphi_A(P_B), \varphi_A(Q_B) \\ \downarrow{\scriptstyle \varphi_B} & & \downarrow{\scriptstyle \varphi'_B} \\ E_B = E/\langle G_B\rangle, \varphi_B(P_A), \varphi_B(Q_A) & \xrightarrow{\varphi'_A} & E_{AB} \cong E_{BA} \cong E_0/\langle G_A, G_B\rangle\,. \end{array}$$

Here, $\{P_A, Q_A\}$ (resp. $\{P_B, Q_B\}$) are public torsion bases for $E_0[A]$ (resp. $E_0[B]$), G_A (resp. G_B) is a generator of a secret subgroup of $E[A]$ (resp. $E[B]$) chosen by Alice (resp. Bob) and $\varphi'_A = \varphi_{B*}\varphi_A$ (resp. $\varphi'_B = \varphi_{A*}\varphi_B$) is the pushforward of φ_A under φ_B (resp. of φ_B under φ_A). In particular, we have $\ker(\varphi'_B) = \varphi_A(\ker(\varphi_B))$, which is the reason why $\varphi_A(P_B)$ and $\varphi_A(Q_B)$ are revealed by Alice (and similarly for Bob).

The prime used is an SIDH prime typically of the form $p = f2^n3^m - 1$ where $2^n \approx 3^m$, and the degrees of the secret isogenies are 2^n and 3^m respectively, so $A = 2^n$ and $B = 3^m$.

To attack SIDH, we can therefore either look at Alice's key, i.e. a secret degree A isogeny where we are given the images of a basis of the B-torsion or Bob's key, i.e. a secret degree B isogeny where we are given the images of a basis of the A-torsion. As such, the degree of the secret isogeny and torsion point order are (A, B) or (B, A) respectively.

Unfortunately, this extra information can be exploited to recover the secret isogenies of both Alice and Bob in polynomial time [4, 19, 21] by application of the following theorem.

Theorem 1 ([21, §6.4]). *Let $\varphi : E_0 \to E$ be a secret degree d isogeny (where d is known) and assume we are given the images of φ on a basis $\{P, Q\}$ of $E_0[N]$, where N and d are assumed smooth and coprime, and $N^2 > 4d$. Let $\mathbb{F}_q$ be the smallest field over which $E_0[N], E_0[d]$ and φ are defined, then the kernel of φ can be computed in a polynomial number of operations in $\mathbb{F}_q$.*

Remark 2. The attack in fact runs as soon as $N^2 > d$, but the output may be ambiguous because $\ker(\varphi)$ may not be uniquely determined by how φ acts on

$E_0[N]$. E.g., if E_0 has j-invariant 0 and $\omega \in \mathrm{End}(E_0)$ denotes an automorphism such that $\omega^2 + \omega + 1 = 0$, then the isogenies $1 \pm \omega : E_0 \to E_0$ both have degree $d = 3$, have different kernels, yet they agree on $E_0[2]$. The bound $N^2 > 4d$ guarantees that φ and hence also $\ker(\varphi)$ is uniquely determined [17, Lem. 3.1].

2.2 M-SIDH

To make the above SIDH-diagram commute, it is sufficient for Bob to know the subgroup $\varphi_A(\ker(\varphi_B))$ and as such it is not necessary to know the exact image of the chosen generator G_B of $\ker(\varphi_B)$. In M-SIDH [15], SIDH is therefore adapted by revealing $\lambda_A\varphi_A(P_B), \lambda_A\varphi_A(Q_B)$ for some secret $\lambda_A \in \mathbb{Z}_B^\times$ chosen by Alice. However, it is not sufficient to just make this simple change, since by the Weil pairing trick mentioned in the introduction it is possible to recover $\lambda_A^2 \bmod B$, which allows to reduce to the case $\lambda_A^2 = 1 \bmod B$. To prevent exhaustive search, this requires to choose a B (similarly for A) such that there are at least 2^s roots of unity with s the security parameter. Using a divide and conquer approach [15], it is even required for both A and B to have $2s$ different prime factors. As such the primes used in M-SIDH are of CSIDH type $p = 4f\prod_{i=1}^{4s}\ell_i - 1$ where the ℓ_i are consecutive odd small primes and one lets

$$A = \prod_{i=1}^{2s} \ell_{2i-1}, \qquad B = \prod_{i=1}^{2s} \ell_{2i}\,.$$

Due to the large number of small primes required, the total size of p is much larger than for SIDH, e.g. the suggested 128-bit parameter set has p of size 5911 bits. The degree of the secret isogeny and torsion point order are (A, B) or (B, A) respectively.

2.3 FESTA

In FESTA [3] the approach is to construct a trapdoor one-way function from the following (somewhat different) commutative diagram:

$$\begin{array}{ccc} E_0, \begin{pmatrix} P_B \\ Q_B \end{pmatrix} & \xrightarrow{\varphi_A} & E_A, \begin{pmatrix} S \\ T \end{pmatrix} = \mathbf{A}\begin{pmatrix} \varphi_A(P_B) \\ \varphi_A(Q_B) \end{pmatrix} \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} \\ E_1, \mathbf{B}\begin{pmatrix} \varphi_1(P_B) \\ \varphi_1(Q_B) \end{pmatrix} & & E_2, \mathbf{B}\begin{pmatrix} \varphi_2(S) \\ \varphi_2(T) \end{pmatrix}. \end{array}$$

The system parameters contain the curve E_0 together with a basis $\{P_B, Q_B\}$ of $E[B]$ where for efficiency reasons $B = 2^b$. The public key of a user consists of the curve E_A and the tuple

$$\begin{pmatrix} S \\ T \end{pmatrix} = \mathbf{A}\begin{pmatrix} \varphi_A(P_B) \\ \varphi_A(Q_B) \end{pmatrix}$$

where $\mathbf{A}$ (part of the private key) is sampled from a commutative subgroup $X \subseteq \mathrm{GL}_2(\mathbb{Z}_B)$. The input to the one-way function then consists of two isogenies φ_1 and φ_2 and a matrix $\mathbf{B}$ which is also sampled from X. The output of the one-way function are the evaluations of the bases $\{P_B, Q_B\}$ under φ_1 and $\{S, T\}$ under φ_2 both multiplied by $\mathbf{B}$. Using the trapdoor information $\mathbf{A}$ and Theorem 1, it is possible to recover the isogeny $\psi = \varphi_2 \circ \varphi_A \circ \hat{\varphi}_1$ from which φ_1, φ_2 and $\mathbf{B}$ follow. The authors of FESTA propose to use for X the group of invertible 2×2 diagonal matrices over $\mathbb{Z}_B$. In particular, $\mathbf{A} = \mathrm{diag}(\lambda_1, \lambda_2)$, and by using the same Weil pairing trick as before, one can reduce to the case $\lambda_2 = \lambda_1^{-1} \bmod B$.

To make the protocol efficient, the authors suggest $B = 2^b$, but also the degrees of $\varphi_A, \varphi_1, \varphi_2$ are taken smooth and coprime. Furthermore, $\deg(\varphi_A) = v^2$ for a smooth v. This results in a CSIDH-type prime of the form $p = f2^b v d_1 d_2 - 1$. For the 128-bit parameter set, the authors suggest $b = 623$, v has 137 bits, d_1 has 257 bits and d_2 has 260 bits, resulting in a prime of size 1292 bits.

Note that to attack FESTA we can consider two scenarios: either we try to recover the private key φ_A (or equivalently $\mathbf{A}$) or we try to invert the one way function by recovering $\varphi_1, \varphi_2, \mathbf{B}$. Both cases are instances of the same problem, where only the degrees of the secret isogenies are slightly different. In particular, in the first case we have to recover a secret degree v^2 isogeny given 2^b-torsion information, where in the second, we need to recover a secret degree d_1 or d_2 isogeny, again given 2^b-torsion information. Note that once $\mathbf{B}$ is derived, the second isogeny follows immediately.

2.4 CSIDH

Unlike the previous protocols, CSIDH works with $\mathbb{F}_p$-rational curves and $\mathbb{F}_p$-rational isogenies. More in detail, CSIDH works on the set of supersingular elliptic curves over $\mathbb{F}_p$ whose ring of $\mathbb{F}_p$-rational endomorphisms is isomorphic to a fixed order $\mathcal{O}$ in the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. It is possible to define a group action of the ideal class group of $\mathcal{O}$ on this set as follows: let $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$ be an ideal class, represented by an ideal $\mathfrak{a} \subseteq \mathcal{O}$ of norm coprime to p. Then the $\mathfrak{a}$-torsion subgroup on a curve E_0 is defined as

$$E_0[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \ker(\alpha),$$

which is finite of order $N(\mathfrak{a}) = \#(\mathcal{O}/\mathfrak{a})$. Thus there exists an elliptic curve E and a separable isogeny $\varphi_{\mathfrak{a}} : E_0 \to E$ with $\ker(\varphi_{\mathfrak{a}}) = E_0[\mathfrak{a}]$, which is unique up to post-composition with an isomorphism. The isomorphism class of E is independent of the choice of the representing ideal $\mathfrak{a}$ and we denote this isomorphism class with $[\mathfrak{a}]E_0$. This approach can be extended to more general oriented curves [11, 20].

To speed-up isogeny computations, p is chosen to be of CSIDH-type, in particular, $p = 4f \prod_{i=1}^{t} \ell_i - 1$ where the ℓ_i are small odd primes. To achieve classical 128-bit security it is sufficient to take p of size 512 bits; however, for post-quantum security p needs to be much larger, e.g. for 128-bit post-quantum security p needs to be of size 4096 bits [9].

As we described in the introduction, CSIDH implicitly leaks a lot of information. Indeed for any $P \in E_0[N]$ that is an eigenvector of π_0 with eigenvalue $\mu \in \mathbb{Z}_N$, we have that $\varphi(P)$ is also an eigenvector of π with eigenvalue μ. So as long as the eigenspace in $E_0[N]$ corresponding to μ is one-dimensional, we obtain $\lambda\varphi(P)$. Note that this reasoning holds for any N for which there is a unique one-dimensional eigenspace with eigenvalue μ, which will be the case as long as N is odd and for each prime factor $\ell \mid N$ we have $\left(\frac{-p}{\ell}\right) = 1$ since the characteristic polynomial of Frobenius is $x^2 + p$. This shows we can take N arbitrary large, and in particular, we are always in the overstretched case.

3 Generalized lollipop attacks

3.1 Strategy

We now detail and generalize the attack strategy from the introduction. Our goal is to recover a secret cyclic isogeny $\varphi : E_0 \to E$ of known degree d, when given bases $\{P, Q\} \subseteq E_0[N]$ and $\{S, T\} \subseteq E[N]$ such that

$$\begin{pmatrix} S \\ T \end{pmatrix} = \mathbf{A} \cdot \varphi \begin{pmatrix} P \\ Q \end{pmatrix}$$

for some secret matrix $\mathbf{A}$ sampled from a public set $X \subseteq \mathrm{GL}_2(\mathbb{Z}_N)$; here, and always from now on, it is assumed that $p \nmid N$. In M-SIDH the set X consists of all invertible scalar matrices, while for the standard instantiation of FESTA it consists of all invertible diagonal matrices. We make use of two auxiliary inputs:

- an isogeny $\sigma_0 : E_0 \to E_0'$ (we denote its degree by s) whose push-forward

$$\sigma := \varphi_* \sigma_0 : E \to E'$$

  under φ is known; equivalently, we know $\varphi(\ker(\sigma_0))$ as a subgroup scheme of E,
- another isogeny $\omega : E_0 \to E_0'$ having the same codomain, of small degree w,

as depicted in Figure 1. For simplicitly, we assume throughout that N, d, s, w are

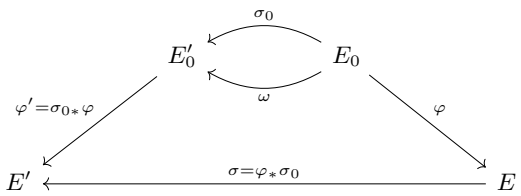


Figure 1. Generalized attack diagram.

pairwise coprime and that $p \nmid dw$. It is allowed that $p \mid s$: indeed, an important special case is where σ_0 is the Frobenius isogeny.

Under suitable "compatibility" conditions, which are discussed in more detail in Section 3.2 below, the attack returns an oracle for evaluating the degree-wd^2 isogeny

$$\psi := \varphi' \circ \omega \circ \hat{\varphi} : E \to E'$$

at any given point. Here φ' denotes the push-forward isogeny $\sigma_{0*}\varphi : E'_0 \to E'$, i.e., the isogeny with kernel $\sigma_0(\ker(\varphi))$ normalized such that $\varphi' \circ \sigma_0 = \sigma \circ \varphi$. If ψ is cyclic then this can be used to recover $\ker(\varphi)$. But even in the non-cyclic case, this typically reveals non-trivial information about φ; see again Section 3.2 for a discussion. The key ingredient is the following lemma, which describes the images of S and T under ψ.

Lemma 3. *Using the above notation, assume that the matrix* $\mathbf{M}$ *such that*

$$(\hat{\sigma}_0 \circ \omega) \begin{pmatrix} P \\ Q \end{pmatrix} = \mathbf{M} \cdot \begin{pmatrix} P \\ Q \end{pmatrix}$$

commutes with every element of X*. Then we have*

$$s \cdot \psi \begin{pmatrix} S \\ T \end{pmatrix} = d \cdot \mathbf{M} \cdot \sigma \begin{pmatrix} S \\ T \end{pmatrix} .$$

Proof. Since $\begin{pmatrix} S \\ T \end{pmatrix} = \mathbf{A} \cdot \varphi \begin{pmatrix} P \\ Q \end{pmatrix}$ and $\hat{\varphi} \circ \varphi = [d]$ we have that

$$\hat{\varphi} \begin{pmatrix} S \\ T \end{pmatrix} = d \cdot \mathbf{A} \cdot \begin{pmatrix} P \\ Q \end{pmatrix} .$$

Furthermore, we have $\varphi' \circ \sigma_0 = \sigma \circ \varphi$ which implies that $[s] \circ \varphi' = \sigma \circ \varphi \circ \hat{\sigma}_0$ and therefore

$$s \cdot (\varphi' \circ \omega \circ \hat{\varphi}) \begin{pmatrix} S \\ T \end{pmatrix} = d \cdot \mathbf{A} \cdot (\sigma \circ \varphi \circ \hat{\sigma}_0 \circ \omega) \begin{pmatrix} P \\ Q \end{pmatrix} = d \cdot \mathbf{A} \cdot \mathbf{M} \cdot (\sigma \circ \varphi) \begin{pmatrix} P \\ Q \end{pmatrix}$$

We thus see that

$$s \cdot \psi \begin{pmatrix} S \\ T \end{pmatrix} = d \cdot \mathbf{A} \cdot \mathbf{M} \cdot \mathbf{A}^{-1} \cdot \sigma \begin{pmatrix} S \\ T \end{pmatrix} , \tag{3}$$

and the lemma follows because $\mathbf{M}$ commutes with every matrix in X, in particular it commutes with $\mathbf{A}$. □

One sees that, whenever the lemma applies, we obtain full knowledge of $\psi(S)$ and $\psi(T)$, because it is assumed that $\gcd(s, N) = 1$. If we then assume that N is smooth and $N^2 > \deg(\psi) = wd^2$, then an application of Theorem 1 yields the desired oracle for evaluating ψ.

Our assumption on σ_0, namely that we know its push-forward by the unknown isogeny φ, is obviously very restrictive. Nevertheless, there are two natural candidates for σ_0, both of which lead to interesting instantiations of our attack strategy:

1. the identity map $\mathrm{id} : E_0 \to E_0$, with push-forward the identity map on E,
2. the Frobenius isogeny
$$\pi_0 : E_0 \to E_0^{(p)},$$
whose push-forward is the Frobenius isogeny from E to $E^{(p)}$,

Other examples are obtained by composing one of the above examples with an isogeny of small degree: then its push-forward can be guessed with a reasonable success probability, which is good enough for our purposes.

Remark 4. If X consists of diagonal matrices,[2] then there is another natural family of isogenies whose push-forwards under φ are known. Indeed, isogenies of the form $E_0 \to E_0/\langle \mu P \rangle$ or $E_0 \to E_0/\langle \mu Q \rangle$ for some $\mu \in \mathbb{Z}$ are pushed-forward to $E \to E/\langle \mu S \rangle$ and $E \to E/\langle \mu T \rangle$, respectively. If X is the set of scalar matrices, as in the case in M-SIDH, then we can even take any isogeny $\sigma_0 : E_0 \to E_0'$ with $\ker(\sigma_0) \subseteq E_0[N]$. However, in these cases s and N are never coprime and Lemma 3 bears only partial information about $\psi(S)$ and $\psi(T)$.

Likewise, for $\mathbf{M}$ to have a reasonable chance of commuting with every matrix in X, the centralizer of X in $\mathrm{GL}_2(\mathbb{Z}_N)$ has to be sufficiently large, and this puts severe restrictions on X. We discuss a few special cases:

1. if $X = \{\text{ scalar matrices }\}$ as is the case in M-SIDH, then the centralizer is all of $\mathrm{GL}_2(\mathbb{Z}_N)$; in other words this condition is void,
2. if $X = \{\text{ diagonal matrices }\}$ as in standard FESTA, then X is its own centralizer. In this case the condition is equivalent to P, Q being eigenvectors of $\hat{\sigma}_0 \circ \omega$ acting on $E_0[N]$,
3. if $X = \{\text{ circulant matrices }\}$, as has also been proposed for use in FESTA [3, Footnote 3], then again X is its own centralizer.

The latter two examples are instances of maximal commutative subgroups of $\mathrm{GL}_2(\mathbb{Z}_N)$. Many further examples can be found in Appendix A, where we give a partial classification of such subgroups.

Remark 5. In the case of diagonal matrices,[3] the condition on $\mathbf{M}$ can be relaxed at the expense of a stronger condition on N. Namely, if P is an eigenvector of $\hat{\sigma}_0 \circ \omega$ then it remains possible to determine $\psi(S)$, even in cases where Q is not an eigenvector. If N is smooth and $N > wd^2$ then this still allows us to obtain the desired evaluation oracle; e.g., if N is a smooth square[4] then one can use a reduction by De Feo et al. [13], the details of which can be found in [5, p. 22]. Of course, the analogous remark applies if Q is an eigenvector, but P not necessarily is.

[2] More generally, a variant of this remark applies whenever X is a so-called *split Cartan subgroup* of $\mathrm{GL}_2(\mathbb{Z}_N)$; see Appendix A.

[3] Here too, a variant of this remark applies if X is a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_N)$.

[4] The general case, i.e. N need not be a square, was solved recently at the workshop "Isogeny Graphs in Cryptography", Banff (Canada) and Bristol (UK), 20–25 August 2023.

3.2 Information retrieved from the attack

Let us sum up the requirements for the attack strategy from Section 3.1 to reveal (at least partial) information about the secret isogeny φ:

- Firstly, the basis $\{P, Q\}$, the isogenies σ_0, ω and the set X should be such that the matrix $\mathbf{M}$ belongs to the centralizer of X in $\mathrm{GL}_2(\mathbb{Z}_N)$, so that Lemma 3 applies.
- Secondly, N should be smooth and larger than wd^2, so that we can invoke Theorem 1.
- Thirdly and most subtly, the isogeny $\psi = \varphi' \circ \omega \circ \hat{\varphi}$ should encode non-trivial information about φ.

We discuss this third point in more detail. The ideal scenario is where ψ is cyclic, in which case we simply recover $\ker(\hat{\varphi})$ as $\ker(\psi)[d]$. A worst case scenario is where $\hat{\sigma}_0 \circ \omega \in \mathbb{Z}$. Indeed, if we assume that σ_0 is cyclic then this implies that $\omega = \sigma_0$ and therefore

$$\psi = \varphi' \circ \omega \circ \hat{\varphi} = \varphi' \circ \sigma_0 \circ \hat{\varphi} = \sigma \circ \varphi \circ \hat{\varphi} = \sigma \circ [d],$$

leaving us clueless about φ (if σ_0 is not cyclic then a similar conclusion applies).

Let us henceforth assume that $\hat{\sigma}_0 \circ \omega$ is cyclic and make a more systematic analysis. Let $d' \mid d$ be maximal such that

$$E[d'] \subseteq \ker(\psi). \tag{4}$$

Let P be a generator of the (as yet unknown) kernel of $\hat{\varphi}$. Because $(\ker(\psi))[d] \cong \mathbb{Z}_{d'} \times \mathbb{Z}_d$, we can compute $d'P$ up to an invertible scalar by taking any order-d point in $\ker(\psi)$ and scaling it by d'. This reveals a degree-d/d' component of $\hat{\varphi}$ emanating from E, and one's task is to close the remaining gap of degree d', as illustrated in Figure 2. Equivalently, the goal is to find $\ker(\varphi)[d']$. Notice that

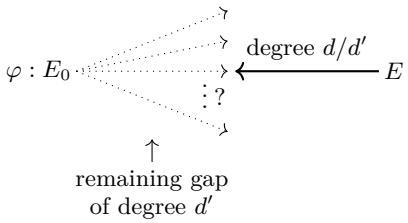


Figure 2. Extracting φ from ψ.

the case $\ker(\psi)$ cyclic corresponds to $d' = 1$.

To proceed, observe that equation (4) is equivalent to

$$\omega(\ker(\varphi))[d'] = \ker(\varphi')[d'] = \sigma_0(\ker(\varphi))[d'],$$

which in turn can be rewritten as

$$(\hat{\sigma}_0 \circ \omega)(\ker(\varphi))[d'] = \ker(\varphi)[d'].$$

Thus from (4) we learn that $(\ker(\varphi))[d']$ is an invariant subspace of $\hat{\sigma}_0 \circ \omega$ acting on $E_0[d']$. This strongly narrows down the options, and we proceed by guessing. For example, if $d = \ell^e$ is a power of an odd prime ℓ, then necessarily $d' = \ell^{e'}$ for some $0 \leq e' \leq e$. Then

- if ℓ splits in $\mathbb{Z}[\hat{\sigma}_0 \circ \omega]$ then possibly $e' > 0$, in which case we are left with exactly two options for $(\ker(\varphi))[d']$, namely the two eigenspaces of $\hat{\sigma}_0 \circ \omega$ acting on $E_0[d']$,
- if ℓ is inert in $\mathbb{Z}[\hat{\sigma}_0 \circ \omega]$, then necessarily $e' = 0$, i.e., $d' = 1$.

Remark 6. In order to avoid too many technicalities, we have ignored the (exceptional) ramified case in our analysis: there we may be left with anything between 0 and $\ell^e + \ell^{e-1}$ options for $(\ker(\varphi))[d']$. For a similar reason, we have omitted the case $\ell = 2$, where there are up to 4 options for $(\ker(\varphi))[d']$ in the split case.

More generally, the number of options for $(\ker(\varphi))[d']$ grows roughly as $O(2^{r'})$ with r' denoting the number of distinct prime factors of d'. So, in the worst case, our strategy involves an exponential number of guesses (e.g. this is the main bottleneck when applying it to CSIDH, we refer to Section 6 for a more elaborate discussion). However, for fixed φ and varying $\hat{\sigma}_0 \circ \omega$, we typically expect r' to be very small. This is based on the following heuristic reasoning. Write

$$d = \ell_1^{e_1} \cdots \ell_r^{e_r}, \qquad d' = \ell_1^{e_1'} \cdots \ell_r^{e_r'} \quad (0 \leq e_i' \leq e_i)$$

as products of distinct prime powers and assume for simplicity that all prime factors ℓ_i are odd. Then r' equals the number of indices i for which $e_i' > 0$, which holds if and only if $(\ker \varphi)[\ell_i]$ happens to be an eigenspace of $\hat{\sigma}_0 \circ \omega$. If ℓ_i splits in $\mathbb{Z}[\hat{\sigma}_0 \circ \omega]$ then there are two such eigenspaces and we estimate the probability for this to happen by $2/(\ell_i + 1)$. If ℓ_i is inert in $\mathbb{Z}[\hat{\sigma}_0 \circ \omega]$, then this cannot happen. Altogether we arrive at an estimated probability of

$$\frac{1}{2} \cdot \frac{2}{\ell_i + 1} + \frac{1}{2} \cdot 0 = \frac{1}{\ell_i + 1}$$

that $e_i' > 0$. So the expected value of r' is

$$\sum_{i=1}^{r} \frac{1}{\ell_i + 1} \leq \sum_{\substack{\text{primes} \\ \ell \leq d}} \frac{1}{\ell} = O(\log \log d), \tag{5}$$

where the last estimate follows e.g. from [23, Thm. 1.10].

Remark 7. A priori, the expected number of guesses is not given by $2^{r'}$ with r' the estimate from (5). Instead, an exact formula for the expected number of

guesses is:

$$\sum_{\mathbf{b}\in\{0,1\}^r} 2^{\#\{\,i\,|\,\mathbf{b}_i=1\,\}} \left(\prod_{\substack{i=1\\ \mathbf{b}_i=0}}^{r} \frac{\ell_i}{\ell_i+1}\right)\left(\prod_{\substack{i=1\\ \mathbf{b}_i=1}}^{r} \frac{1}{\ell_i+1}\right) = \prod_{i=1}^{r} \frac{\ell_i+2}{\ell_i+1}.$$

This can be estimated as

$$\prod_{\substack{\text{primes}\\ \ell\leq d}} \frac{\ell+2}{\ell+1} \leq \prod_{\substack{\text{primes}\\ \ell\leq d}} \frac{\ell}{\ell-1} = O(\log d)$$

by Mertens' formula [23, Thm. 1.12].

3.3 Comparison to lollipop attack

If $\sigma_0 : E_0 \to E_0$ is just the identity map, then ω must be an endomorphism and

$$\psi = \varphi \circ \omega \circ \hat{\varphi}$$

is the corresponding "lollipop endomorphism" on E; this nomenclature was popularized by [14]. For $X = \{\,\text{scalar matrices}\,\}$ we recover the attack on M-SIDH as outlined in [15, §4.2-4.3]. Therefore, the strategy from Section 3.1 should be viewed as a generalization of this lollipop attack to arbitrary sets X and arbitrary instances of σ_0.

Let us highlight the role of σ_0. In theory, it would also be possible to just apply the lollipop attack to the endomorphism

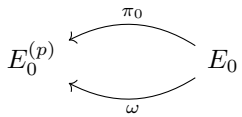
$$\omega' = \hat{\sigma}_0 \circ \omega \in \mathrm{End}(E_0).$$

But then we would need that $N^2 > swd^2$, rather than just $N^2 > wd^2$. So the crucial observation is that components of ω' whose push-forward under φ are known (σ_0 in this case) do not contribute to the degree of ψ and thereby lead to an improvement on the lower bound on N.

Example 8. One clear instance where one can take $\sigma_0 = \pi_0$ is when the starting curve E_0 is defined over $\mathbb{F}_p$. In this case π_0 is an endomorphism and one can simply take $\omega = \mathrm{id}$, so that

$$\psi = \varphi^{(p)} \circ \hat{\varphi}.$$

Note that, when compared to the lollipop attack applied to $\omega = \pi_0$, the degree of ψ drops from pd^2 to d^2. This corresponds to the attack strategy described in the introduction. In turn, the insertion of an endomorphism ω is a special case of the more general situation where E_0 is not necessarily defined over $\mathbb{F}_p$ but is connected to its Frobenius conjugate via a small-to-moderate degree isogeny ω:



Such curves were considered, for instance, in [10].

4 M-SIDH

In this section we apply our attack to M-SIDH, where we analyze the different choices for σ_0. Recall that $S = \lambda\varphi(P)$ and $T = \lambda\varphi(Q)$ for a basis $\{P, Q\}$ of $E[N]$ with $\lambda \in \mathbb{Z}_N^\times$ and $d = \deg(\varphi)$.

4.1 Case $\sigma_0 = \mathrm{id}$

Let ω be an endomorphism on E_0 and set $\psi = \varphi \circ \omega \circ \hat{\varphi}$, then Lemma 3 implies

$$\psi \begin{pmatrix} S \\ T \end{pmatrix} = d \cdot \mathbf{M} \begin{pmatrix} S \\ T \end{pmatrix}$$

with $\mathbf{M}$ the (transpose of the) matrix of ω acting on $E_0[N]$ with respect to the basis $\{P, Q\}$. Using our attack we obtain an oracle for evaluating ψ as soon as $N > d\sqrt{w}$. If w is sufficiently small, then this condition is likely satisfied for either Alice's or Bob's secret isogeny. Unless $\omega \equiv [\lambda] \bmod [N]$ in $\mathrm{End}(E_0)$ for some $\lambda \in \mathbb{Z}$, the oracle can then be used to extract non-trivial information about φ. In general, one simply expects that ψ is a cyclic isogeny revealing all of $\ker(\hat{\varphi})$ and hence $\ker(\varphi)$. Thus as soon as E_0 comes equipped with a small non-scalar endomorphism then one should consider M-SIDH broken. This is precisely the attack described in [15, §4.2-4.3]. Similarly, by focusing on $\hat{\varphi} : E \to E_0$ rather than on $\varphi : E_0 \to E$, the same conclusion applies if E carries a small non-scalar endomorphism.

Remark 9. If the endomorphism ring of E_0 (resp. E) is known and we are in the overstretched case where $N/d \gtrapprox p^{1/3}$, then we can run the attack with a non-scalar endomorphism ω on E_0 (resp. on E) of degree about $p^{2/3}$, which exists in view of [18, Prop. B.5] and can be computed using lattice reduction.[5]

4.2 Case $\sigma_0 = \pi_0$

If the curve E_0 is $\mathbb{F}_p$-rational, we can take $\omega = \mathrm{id}$ and consider $\psi = \varphi^{(p)} \circ \hat{\varphi}$. Since $p \nmid N$ by assumption, Lemma 3 implies

$$\psi \begin{pmatrix} S \\ T \end{pmatrix} = (p^{-1}d \bmod N) \cdot \mathbf{M} \cdot \pi \begin{pmatrix} S \\ T \end{pmatrix}$$

with $\pi : E \to E^{(p)}$ the Frobenius isogeny and $\mathbf{M}$ the (transpose of the) matrix of $\hat{\pi}_0$ acting on $E_0[N]$ with respect to the basis $\{P, Q\}$. Note that

$$p^{-1}\mathbf{M} = \mathbf{M}_{\pi_0}^{-1},$$

so this confirms equation (1). As above, we thus obtain an oracle for evaluating ψ as soon as $N > d$; recall that in M-SIDH this condition is satisfied for either

[5] A similar remark is made in [15, §4.3] but their claim that ω can be taken of degree about $p^{1/2}$ seems slightly overoptimistic.

Alice's or Bob's secret isogeny. In general, one expects that ψ is a cyclic isogeny revealing all of $\ker(\varphi)$. Consequently, one should consider M-SIDH insecure as soon as E_0 is defined over $\mathbb{F}_p$. Again, by focusing on $\hat{\varphi} : E \to E_0$ instead, the same conclusion applies in case E is defined over $\mathbb{F}_p$.

More general, we can consider the case where E_0 is not $\mathbb{F}_p$-rational, but such that there exists a low degree isogeny $\omega : E_0 \to E_0^{(p)}$. The attack then results in an oracle to evaluate $\psi = \varphi^{(p)} \circ \omega \circ \hat{\varphi}$ as long as $N > d\sqrt{w}$. As such, if E_0 is close to its Frobenius conjugate $E_0^{(p)}$, i.e. w is small enough, then M-SIDH is also insecure. Once again, we arrive at the same conclusion in case E and $E^{(p)}$ are connected by a small-degree isogeny.

4.3 Backdoors

In this section we analyze how easy it would be for an attacker to backdoor M-SIDH by generating rigged system parameters and whether these backdoors can be detected or avoided altogether. The general idea is to generate system parameters E_0, P_B, Q_B which are a short distance removed, i.e. via a somewhat low degree isogeny ϵ, from one of the weak instances described above. Note that due to the symmetry of M-SIDH, i.e. by looking at the dual, the domain and co-domain are swapped, the same checks have to be performed for the co-domain curve E.

In [15, §7.1] the authors analyzed the requirements on the starting curve E_0 for M-SIDH to be secure and concluded that any curve E_0 without a small endomorphism is sufficient. Since a random $\mathbb{F}_p$-rational supersingular elliptic curve will not admit small endomorphisms, but still succumbs to our attack, this is clearly not sufficient. Furthermore, since the starting curve is part of the system parameters, for efficiency reasons, it might be tempting to organize a distributed random walk in the $\mathbb{F}_p$-isogeny graph. As we have shown, this is a bad idea.

Given a starting curve E_0 which is generated by a third party (trusted or not), detecting a possible backdoor amounts to verifying that E_0 and $E_0^{(p)}$ are not close in the $\mathbb{F}_{p^2}$-isogeny graph. Let $\theta : E_0 \to E_0^{(p)}$ be a connecting isogeny of degree t, then the composition $\hat{\pi}_0 \circ \theta$ is an endomorphism on E_0 of degree $t \cdot p$. Unfortunately, we are not aware of an efficient test for the existence of such endomorphism. The only (trivial) possibility seems to be to test whether $\Phi_k(j(E_0), j(E_0)^p) = 0$ for all $k = 1, \ldots, U$. The bound U depends on the difference between the degree of the isogenies φ_A (resp. φ_B) and the order of P_B, Q_B (resp. P_A, Q_A). To illustrate, if we are trying to recover φ_A, then the isogeny $\psi = \varphi_A^{(p)} \circ \theta \circ \varphi_A$ has degree $A^2 t$ with $A = \deg(\varphi_A)$ and we thus require $B^2 > A^2 t$ or equivalently, $(B/A)^2 > t$. As such, we require to test at least up to

$$U \geq \max\{\frac{A^2}{B^2}, \frac{B^2}{A^2}\}.$$

To make this test efficient, it is therefore beneficial to take A as close to B as possible, which corresponds to the parameter selection in [15]. In particular, for

the largest M-SIDH parameter set, we need to test existence of isogenies up to degree $U < 823$.

Finally, the authors suggest that the curve is generated using an MPC protocol as in [2], where a random supersingular curve is generated by n parties in a round-robin manner, i.e. party i executes a secret isogeny walk from E_{i-1} to E_i, where party 1 starts from a known supersingular elliptic curve E_0. Furthermore, each party needs to prove that they really know a path from E_{i-1} to E_i. The question now becomes whether the last party can force the walk to go through a curve E which is close to its Frobenius conjugate $E^{(p)}$. Since we assume at least one honest party preceding the last one, it is clear that for party n the curve E_{n-1} is a random supersingular elliptic curve. According to [8, Lem. 6], the number of (isomorphism classes of) supersingular elliptic curves such that E and $E^{(p)}$ are connected by an isogeny of degree up to d is bounded by $\tilde{O}(\sqrt{d^3 p})$. The probability of party n being able to force such a curve is therefore negligible.

In conclusion: using an MPC protocol as in [2] to execute an isogeny walk in the full $\mathbb{F}_{p^2}$-isogeny graph, will result in a non-backdoored curve with overwhelming probability. As an added measure, one can run the explicit test described above.

5 FESTA

To apply our attack to FESTA, in view of Remark 5 we require at least one of the basis points to be an eigenvector of $\hat{\sigma}_0 \circ \omega$ where σ_0 is either the identity or Frobenius and ω is a small degree endomorphism. Recall that in FESTA the torsion point order is given by $B = 2^b$ and our attack recovers $\psi = \sigma_{0*}\varphi \circ \omega \circ \hat{\varphi}$ as long as $B > d\sqrt{w}$, in case we know the images of a full basis, or $B > d^2 w$, in case we only know the image of a single point.

In this section we analyze how many such ω and *different* eigenspaces can exist for the curve $E_0 : y^2 = x^3 + 6x^2 + x$ over $\mathbb{F}_p$ used in the FESTA implementation [3]. Since E_0 is 2-isogenous to the elliptic curve $E_1 : y^2 = x^3 + x$ via an isogeny θ with $\ker\theta = \langle(0,0)\rangle$, and since the endomorphism ring of E_1 is well-known,[6] we can compute the following $\mathbb{Z}$-module basis of $\mathrm{End}(E_0)$:

$$\mathrm{id},\ \frac{\pi_0 - [1]}{2},\ \mathbf{i} - \mathbf{i}\pi_0,\ \frac{\mathbf{i} + \mathbf{i}\pi_0}{4},$$

where $\mathbf{i} = \sqrt{-1}$ and π_0 the Frobenius endomorphism. Note that $\mathbf{i}$ itself is not an endomorphism on E_0, but is an endomorphism on E_1. As such we obtain the endomorphism $2\mathbf{i} = \hat{\theta} \circ \mathbf{i} \circ \theta$ on E_0.

To simplify matters we will work with the subring generated by $\mathrm{id}, \pi_0, 2\mathbf{i}, 2\mathbf{i}\pi_0$, which has index 16 in $\mathrm{End}(E_0)$. Since $\deg(\pi_0) = p$ and we require $w = \deg(\omega)$ to be of moderately small degree (note that in the overstretched case we can allow for combinations with π_0), we are thus limited to choosing ω of the form $a + 2b\mathbf{i}$ which has degree $a^2 + 4b^2$.

[6] See e.g. Section 6 for an explicit basis.

To illustrate this for the 128-bit secure parameter set, we have $B = 2^{632}$ and d has 273 bits, which allows ω of degree up to 2^{718} assuming we know images of a full basis and ω of degree up to 2^{86} if we only know the image of a single point.

5.1 Case $\sigma_0 = \mathrm{id}$

We have to analyze the eigenspaces of $\omega = \alpha + 2\beta\mathbf{i}$ with $\alpha, \beta \in \mathbb{Z}$. However it is easy to see that if P is an eigenvector of such ω with eigenvalue μ, then if $\gcd(\beta, B) = 1$, P is also an eigenvector of $2\mathbf{i}$ with eigenvalue $(\mu - \alpha)/\beta \bmod B$. As such the different choices for ω do not result in distinct eigenspaces, and only the eigenspaces of $2\mathbf{i}$ are weak.

5.2 Case $\sigma_0 = \pi_0$

We have to analyze the eigenspaces of $\hat{\pi}_0 \circ \omega = \hat{\pi}_0 \circ (\alpha + 2\beta\mathbf{i})$. Since $\pi_0^2 = [-p]$ on E_0, we have $\hat{\pi}_0 = -\pi_0$, so it suffices to analyze the eigenspaces of $\pi_0 \circ (\alpha + 2\beta\mathbf{i})$.

Assume for now that B is odd (the case $B = 2^n$ is analyzed below). Let $\{U, V\}$ be a basis of eigenvectors of π_0 on $E_0[B]$, i.e. $\pi_0(U) = U$ and $\pi_0(V) = -V$ (here we used $p \equiv -1 \bmod B$ as in FESTA). Since π_0 and $2\mathbf{i}$ anti-commute, we can in fact take $V = 2\mathbf{i}(U)$, which indeed satisfies $\pi_0(V) = -V$ and has the same order as U (here we use B odd). Note that we also have the equality $2\mathbf{i}(V) = -4U$.

Assume that $P \in E_0[B]$ is an eigenvector of $\pi_0 \circ (\alpha + 2\beta\mathbf{i})$ of exact order B, then using the basis $\{U, V\}$ of $E[B]$, we can express $P = cU + dV$ with $c, d \in \mathbb{Z}_B$ and at least one of c, d is a unit in $\mathbb{Z}_B$. Assume without loss of generality that this is c, then after rescaling by $c^{-1} \bmod B$, we can assume P is of the form $P = U + aV$ with $a \in \mathbb{Z}_B$. Note that by rescaling we are now counting different eigenspaces instead of eigenvectors, in particular, each a gives rise to a whole different eigenspace (and thus $\phi(B)$ different eigenvectors of exact order B, where ϕ denotes the Euler-phi function). To deal with the case that P has order $B'|B$ with $B' < B$, we can simply replace B by B', U by $(B/B')U$ and V by $(B/B')V$.

Assume that the eigenvalue corresponding to P is μ then using $V = 2\mathbf{i}(U)$ and $2\mathbf{i}(V) = -4U$ we have

$$\pi_0 \circ (\alpha + 2\beta\mathbf{i})(P) = (\alpha - 4a\beta)U + (-a\alpha - \beta)V = \mu(U + aV)\,.$$

This is equivalent with

$$4a^2\beta - 2a\alpha - \beta \equiv 0 \bmod B\,.$$

For every choice of α and β we therefore get a quadratic equation for a with discriminant $\Delta = 4\alpha^2 + 16\beta^2$.

Case $B = \ell^n$ with ℓ an odd prime Assume first that $B = \ell^n$ for an odd prime ℓ, then for β a unit in $\mathbb{Z}_B$, this equation will have two different solutions

for a exactly when $\left(\frac{\Delta}{\ell}\right) = 1$ which are given by

$$a_\pm = \frac{\alpha \pm \sqrt{\alpha^2 + 4\beta^2}}{4\beta} = \frac{(\alpha/2\beta) \pm \sqrt{(\alpha/2\beta)^2 + 1}}{2} \bmod B\,.$$

Note that the solutions for a result in two different eigenspaces, one corresponding to a_+ and one corresponding to a_- and that the one fully determines the other. In particular, the eigenspaces come in pairs corresponding to $\{a_+, a_-\}$.

Assume we now consider the attack where the images of a full basis are required, then w is bounded by $w = \deg(\omega) = \alpha^2 + 4\beta^2 < (B/d)^2$. To estimate the total number of pairs of weak eigenspaces, we therefore simply need to compute the number of *different* values for a above where α, β vary *inside* the ellipse $x^2 + 4y^2 = (B/d)^2$. Ignoring (small) constants, the number of such pairs is given by $(B/d)^2$. However, as shown above, the value of a is really determined by $\alpha/2\beta \bmod B$. As such we need to distinguish 2 cases: if $d > \sqrt{B}$, then up to a small constant, the number of values for a really is $(B/d)^2$, however, when $d < \sqrt{B}$ the number of values for a is simply B. This shows that the total number of weak eigenspaces is, up to a small constant, given by

$$\min\{\frac{B^2}{d^2}, B\}\,.$$

Since the total number of eigenspaces is given by B^2, we conclude that the proportion of weak eigenspaces for FESTA in the full basis attack scenario is $O(\min\{\frac{1}{d^2}, \frac{1}{B}\})$.

We can do a similar analysis for the case where we want to run the attack with the image of only a single point, following Remark 5. The main difference is now that the bound on w is changed to $w = \deg(\omega) = \alpha^2 + 4\beta^2 < B/d^2$. Instead of counting the number of pairs of eigenspaces, we now simply count the number of eigenspaces. As before, we need to compute the number of *different* values for a above where α, β vary *inside* the ellipse $x^2 + 4y^2 = B/d^2$ (note the right hand side is different from before). Up to a small constant, this number is given by B/d^2. Note that for $d > \sqrt{B}$ there are no solutions, and otherwise there are B/d^2 (up to a small constant). Given that there are B different eigenspaces in total, the proportion of weak eigenspaces for FESTA in the single image point attack scenario is $O(1/d^2)$.

Case $B = 2^n$ with $n > 3$ The overall reasoning remains exactly the same, with a few small changes. The first change is that since $E[2]$ is already rational over $\mathbb{F}_p$ in FESTA, we will only be able to select U of order $B/2$. Furthermore, by construction $V = 2\mathbf{i}(U)$ only has order $B' = B/8$ (note that the $\deg(2\mathbf{i}) = 4$, so this is the worst that can happen). We thus consider the basis $U' = 4U$ and V for $E[B']$. Note that we now have the equality $2\mathbf{i}(V) = -U'$. Considering eigenvectors of the form $P = U' + aV \in E[B']$ with eigenvalue μ, we get

$$\pi_0 \circ (\alpha + 2\beta\mathbf{i})(P) = (\alpha - a\beta)U' + (-a\alpha - 4\beta)V = \mu(U' + aV)\,.$$

The quadratic equation for a thus also changes slightly, in that a now has to satisfy:

$$a^2\beta - 2a\alpha - 4\beta = 0 \bmod B' .$$

For β a unit, i.e. $\beta \not\equiv 0 \bmod 2$, it is easy to verify that the above equation will have no solutions. For $\beta \equiv 0 \bmod 2$, we can set $\beta' = \beta/2$ and obtain the equivalent equation:

$$a^2\beta' - a\alpha - 4\beta' = 0 \bmod B'/2 .$$

It is easy to check that this equation will have 2 solutions modulo $B'/2$ whenever $\beta' \equiv \alpha \bmod 2$ and no solutions otherwise.

The remainder of the analysis now remains exactly the same, since the different solutions are fully determined by α/β, so up to a small constant, it suffices to compute the number of such tuples inside the ellipses $x^2 + 4y^2 = B'^2/d^2$ and $x^2 + 4y^2 = B'/d^2$ exactly as before. As such, also for $B = 2^n$, the proportion of weak eigenspaces for FESTA is again $O(\min\{\frac{1}{d^2}, \frac{1}{B}\})$ in the full basis attack scenario and $O(1/d^2)$ in the single image point attack scenario.

5.3 Backdoors

The general approach of introducing a backdoor into FESTA is similar to the M-SIDH case in that an attacker generates system parameters E_0, P_B, Q_B which are obtained as the image under a low degree isogeny ε of one of the weak instances identified above. In particular, let E_w, P_w, Q_w be a weak instance for FESTA, then $E_0 = \varepsilon(E_w)$, $P_B = \varepsilon(P_w)$ and $Q_B = \varepsilon(Q_w)$. The attack then proceeds to recover $\varepsilon \circ \varphi$, which is possible as long as $B^2 > e^2d^2w$ with $e = \deg(\varepsilon)$. Assuming that the weak basis is optimal, i.e. eigenvectors of Frobenius, we have $w = 1$ and so the backdoor can tolerate isogenies ε up to degree B/d which in FESTA is very large. If the endomorphism ring of E_0 is known or given, then one can proceed exactly as above to test whether the basis is weak; however, when the endomorphism ring of E_0 is unknown, then it is near impossible to verify whether FESTA has been backdoored since the degree of ε can be so large.

A possible, easy solution however is the following: as shown above, the proportion of weak bases for a given curve is on the order of $O(1/d^2)$ which is very small. Therefore, given system parameters E_0, P_B, Q_B it suffices to publicly rerandomize the basis, which with overwhelming probability will result in a basis which no longer is weak. Another possible solution, as done in the FESTA implementation, is to obtain P_B, Q_B deterministically using a hash function to the elliptic curve E_0 such as described in [24]. The paranoid user can rerandomize the basis themselves and include these as part of their public key.

Finally, we note that due to the symmetry of FESTA, i.e. by looking at the dual, the domain and co-domain are swapped, the same checks/countermeasures have to be performed for the co-domain curve E.

5.4 Overstretched FESTA

It is natural to ask whether, given any two points P and Q, it is always possible to construct an endomorphism ω such that P and Q become eigenvectors, and what the expected degree of such ω would be. To analyze this, we consider what can be expected for E_0 a sufficiently general supersingular elliptic curve over $\mathbb{F}_{p^2}$ with known endomorphism ring and $\{P, Q\}$ a sufficiently general basis of $E_0[B]$. Using lattice reduction we can find a $\mathbb{Z}$-basis

$$\mathrm{id}, \omega_1, \omega_2, \omega_3 \in \mathrm{End}(E_0)$$

with $\deg(\omega_i) \approx p^{2/3}$ for all i; see [18, Prop. B.5]. Writing $\mathbf{M}_i$ for the matrix of ω_i acting on $E_0[B]$ with respect to $\{P, Q\}$, we hope to find scalars $\lambda_i \in \mathbb{Z}$ such that

$$\lambda_1 \mathbf{M}_1 + \lambda_2 \mathbf{M}_2 + \lambda_3 \mathbf{M}_3 \tag{6}$$

is diagonal (and non-scalar). The proportion of diagonal matrices in $\mathbb{Z}_B^{2\times 2}$ is $1/B^2$, so we expect that we can take $|\lambda_i| \leq B^{2/3}$, and then $w = \deg(\omega) = \deg(\lambda_1\omega_1 + \lambda_2\omega_2 + \lambda_3\omega_3)$ is in $O(p^{2/3}B^{4/3})$. In conclusion, as soon as $B \gtrapprox pd^3$, we expect being able to find a degree-w endomorphism ω of which P and Q are eigenvectors and such that $B > d\sqrt{w}$, as required for the attack. Note that the condition $B \gtrapprox pd^3$, implies that the B-torsion cannot be $\mathbb{F}_{p^2}$-rational as done in FESTA, so this attack really only concerns an overstretched case and does not apply to FESTA itself.

6 CSIDH

We now discuss CSIDH in its known-degree variant (e.g., the dummy-free variant from [7, §5] with $m = 1$). Concretely, our secret isogeny φ is a horizontal isogeny of known degree d connecting two supersingular elliptic curves E_0, E over $\mathbb{F}_p$. As discussed before, for bases $\{P, Q\} \subseteq E_0[N]$, $\{S, T\} \subseteq E[N]$ consisting of Frobenius eigenvectors we know that

$$\begin{pmatrix} S \\ T \end{pmatrix} = \mathbf{D} \cdot \varphi \begin{pmatrix} P \\ Q \end{pmatrix}$$

for some unknown diagonal matrix $\mathbf{D} \in \mathrm{GL}_2(\mathbb{Z}_N)$, where N can be taken arbitrarily large. Note that the eigenvalues corresponding to P, Q are necessarily of the form $\mu, -\mu$ since the characteristic polynomial of Frobenius is $x^2 + p$.

In order to apply our attack strategy, we wish to find $\sigma_0 \in \{\mathrm{id}, \pi_0\}$ and $\omega \in \mathrm{End}(E_0)$ such that:

- the matrix $\mathbf{M}$ of $\hat{\sigma}_0 \circ \omega$ acting on $E_0[N]$ with respect to the basis $\{P, Q\}$ is diagonal,
- $N^2 > wd^2$, where $w = \deg(\omega)$.

We will show that for

$$E_0 : y^2 = x^3 + x \text{ over } \mathbb{F}_p \text{ with } p \equiv 3 \bmod 8 \tag{7}$$

(as is the setting for the original CSIDH proposal [6]) these conditions imply

$$(\hat{\sigma}_0 \circ \omega)(\ker(\varphi)) = \ker(\varphi) \tag{8}$$

so that, using the notation from Section 3.2, we are always in the case $d' = d$. Consequently, our attack strategy comes with $O(2^r)$ guesses, where r denotes the number of distinct prime factors of d, and therefore does not offer any improvement over existing attacks.

Our belief is that the same conclusions apply to any starting curve over any finite prime field,[7] but the discussion becomes more technical. The two features of (7) that make life easier are:

- N is odd, because 2 does not split in $\mathbb{Q}(\sqrt{-p})$,
- the endomorphism ring of E_0 is easy to handle; namely as a $\mathbb{Z}$-module it is generated by
$$[1],\ \frac{\mathbf{i} + \pi_0}{2},\ \pi_0,\ \frac{[1] + \mathbf{i}\pi_0}{2}$$
with $\mathbf{i} : (x, y) \mapsto (-x, \sqrt{-1}y)$ such that $\mathbf{i}^2 = [-1]$.

It suffices to concentrate on the case $\sigma_0 = \mathrm{id}$. Indeed, the matrix of an endomorphism ω with respect to $\{P, Q\}$ is diagonal if and only if the matrix of $\hat{\pi}_0 \circ \omega = -\pi_0 \circ \omega$ with respect to $\{P, Q\}$ is diagonal. Similarly, the equality from (8) holds for $\sigma_0 = \pi_0$ if and only if it holds for $\sigma_0 = \mathrm{id}$.

Then the main observation is that $\mathbf{i}$ swaps the eigenspaces $\langle P \rangle$ and $\langle Q \rangle$. Indeed, this follows from

$$\pi_0(\mathbf{i}(P)) = -\mathbf{i}(\pi_0(P)) = -\mu\mathbf{i}(P).$$

Consequently, the matrix of $\mathbf{i}$ with respect to $\{P, Q\}$ is anti-diagonal. Likewise, also the matrix of $\mathbf{i}\pi_0$ with respect to $\{P, Q\}$ is anti-diagonal. This means that if we want the matrix of

$$\omega = a_1 + a_2\frac{\mathbf{i} + \pi_0}{2} + a_3\pi_0 + a_4\frac{1 + \mathbf{i}\pi_0}{2} = a_1 + \frac{a_4}{2} + \frac{a_2}{2}\mathbf{i} + (a_3 + \frac{a_2}{2})\pi_0 + \frac{a_4}{2}\mathbf{i}\pi_0$$

with respect to $\{P, Q\}$ to be diagonal, then

$$a_2\mathbf{i} + a_4\mathbf{i}\pi_0 = (a_2 - a_4\pi_0)\mathbf{i}$$

should act as the zero map on $\langle P, Q \rangle = E_0[N]$. By construction π_0 has distinct eigenvalues modulo every prime factor of N, so this can only happen if $a_2 \equiv a_4 \equiv 0 \bmod N$. If $a_2 = a_4 = 0$ then ω is a linear combination of 1 and π_0, from

[7] Or even more generally: to arbitrary orientations.

which it readily follows that $\omega(\ker(\varphi)) = \ker(\varphi)$. On the other hand, as soon as one of a_2, a_4 is non-zero, we find that

$$w \geq \frac{\deg(a_2\mathbf{i} + a_4\mathbf{i}\pi_0)}{4} = \frac{a_2^2 + pa_4^2}{4} \geq N^2/4$$

and therefore $N^2 \leq wd^2$: a contradiction (here we have used that $d > 1$, which can of course be assumed without loss of generality).

Remark 10. According to Remark 5, an alternative strategy is to look for $\omega \in \mathrm{End}(E_0)$ such that P is an eigenvector of $\hat{\sigma}_0 \circ \omega$, but Q not necessarily is; recall that the bound $N^2 > wd^2$ strengthens to $N > wd^2$ in this case. The analysis is similar, except that now we run into the conclusion that $(a_2 - a_4\pi_0)\mathbf{i}$ should vanish on $\langle P \rangle$, rather than on all of $E_0[N]$. Equivalently, this means that $a_2 - a_4\pi_0$ should vanish on $\langle Q \rangle$, or in other words that $a_2 + a_4\mu \equiv 0 \bmod N$. As before, we have

$$w \geq \frac{a_2^2 + pa_4^2}{4}$$

where now we observe that the numerator of the right-hand side is divisible by N because $a_2^2 + pa_4^2 \equiv (\mu^2 + p)a_4^2 \equiv 0 \bmod N$. Here we have used that $\mu^2 + p \equiv 0 \bmod N$ because μ is an eigenvalue of Frobenius mod N. We conclude: if $a_2 = a_4 = 0$ then $\omega \in \mathbb{Z}[\pi_0]$, else $w \geq N/4$ and therefore $N \leq wd^2$.

References

[1] Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, David Jao, Brian Koziel, Brian LaMacchia, Patrick Longa, et al. Supersingular isogeny key encapsulation. *Submission to the NIST Post-Quantum Standardization project*, 152:154–155, 2017.

[2] Andrea Basso, Giulio Codogni, Deirdre Connolly, Luca De Feo, Tako Boris Fouotsa, Guido Maria Lido, Travis Morrison, Lorenz Panny, Sikhar Patranabis, and Benjamin Wesolowski. Supersingular curves you can trust. In *Eurocrypt 2023 Pt. 2*, volume 14005 of *Lecture Notes in Computer Science*, pages 405–437. Springer, 2023.

[3] Andrea Basso, Luciano Maino, and Giacomo Pope. FESTA: Fast encryption from supersingular torsion attacks. To appear at Asiacrypt 2023. Preprint available at https://eprint.iacr.org/2023/660.

[4] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In *Eurocrypt 2023 Pt. 5*, volume 14008 of *Lecture Notes in Computer Science*, pages 423–447. Springer, 2023.

[5] Wouter Castryck, Marc Houben, Simon-Philipp Merz, Marzio Mula, Sam van Buuren, and Frederik Vercauteren. Weak instances of class group action based cryptography via self-pairings. In *Crypto Pt. 3*, volume 14083 of *Lecture Notes in Computer Science*, pages 762–792. Springer, 2023.

[6] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In *Asiacrypt Pt. 3*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018.

[7] Daniel Cervantes-Vázquez, Mathilde Chenu, Jesús-Javier Chi-Domínguez, Luca De Feo, Francisco Rodríguez-Henríquez, and Benjamin Smith. Stronger and faster sidechannel protections for CSIDH. In *Latincrypt*, volume 11774 of *Lecture Notes in Computer Science*, pages 173–193. Springer, 2019.
[8] Denis Xavier Charles, Kristin E. Lauter, and Eyal Z. Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, 2009.
[9] Jorge Chávez-Saab, Jesús-Javier Chi-Domínguez, Samuel Jaques, and Francisco Rodríguez-Henríquez. The SQALE of CSIDH: sublinear Vélu quantum-resistant isogeny action with low exponents. *Journal of Cryptographic Engineering*, 12(3):349–368, 2022.
[10] Mathilde Chenu and Benjamin Smith. Higher-degree supersingular group actions. *Mathematical Cryptology*, 1(2):85–101, 2022.
[11] Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. *Journal of Mathematical Cryptolology*, 14(1):414–437, 2020.
[12] Luca De Feo. Mathematics of isogeny based cryptography, 2017.
[13] Luca De Feo et al. Modular isogeny problems. Private communication.
[14] Victoria de Quehen, Péter Kutas, Chris Leonardi, Chloe Martindale, Lorenz Panny, Christophe Petit, and Katherine E. Stange. Improved torsion-point attacks on SIDH variants. In *Crypto Pt. 3*, volume 12827 of *Lecture Notes in Computer Science*, pages 432–470. Springer, 2021.
[15] Tako Boris Fouotsa, Tomoki Moriya, and Christophe Petit. M-SIDH and MD-SIDH: countering SIDH attacks by masking information. In *Eurocrypt Pt. 5*, volume 14008 of *Lecture Notes in Computer Science*, pages 282–309. Springer, 2023.
[16] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *PQCrypto 2011*, volume 7071 of *Lecture Notes in Computer Science*, pages 19–34. Springer, 2011.
[17] David Jao and David Urbanik. Sok: The problem landscape of SIDH. In *Proceedings of the 5th ACM on ASIA Public-Key Cryptography Workshop*, pages 53–60. ACM, 2018.
[18] Jonathan Love and Dan Boneh. Supersingular curves with small non-integer endomorphisms. In *ANTS-XIV*, volume 4 of *Open Book Series*, pages 7–22. MSP, 2020.
[19] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery attack on SIDH. In *Eurocrypt 2023 Pt. 5*, volume 14008 of *Lecture Notes in Computer Science*, pages 448–471. Springer, 2023.
[20] Hiroshi Onuki. On oriented supersingular elliptic curves. *Finite Fields and Their Applications*, 69, 2021. Article id: 101777.
[21] Damien Robert. Breaking SIDH in polynomial time. In *Eurocrypt 2023 Pt. 5*, volume 14008 of *Lecture Notes in Computer Science*, pages 472–503. Springer, 2023.
[22] Jean-Pierre Serre. *Lectures on the Mordell-Weil Theorem*, volume E15 of *Aspects of Mathematics*. Springer Fachmedien Wiesbaden (orig. Vieweg & Sohn), third edition, 1997.
[23] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, third edition, 2015.
[24] Gustavo H. Zanon, Marcos A. Simplicio, Geovandro C. Pereira, Javad Doliskani, and Paulo S. Barreto. Faster key compression for isogeny-based cryptosystems. *IEEE Transactions on Computers*, 68(5):688–701, 2019.

A Maximal commutative subgroups of $\mathbf{GL_2}(\mathbb{Z}_N)$

This appendix contains a partial classification of the maximal commutative subgroups of $\mathrm{GL}_2(\mathbb{Z}_N)$. The classification seems classical in case N is a prime number, but we could not find a reference that deals with the general case, where various subtleties arise, see for instance Example 12 below. Maximal commutative subgroups of $\mathrm{GL}_2(\mathbb{Z}_N)$ are natural candidates for the set X from Section 3.1, and they can also be used as substitutes for $X = \{\,\text{diagonal matrices}\,\}$ in FESTA [3]. By the Chinese Remainder Theorem, it suffices to concentrate on the case $N = \ell^e$ for some prime number ℓ.

Free maximal commutative subalgebras

We first study maximal commutative sub*algebras* $\mathcal{A} \subseteq \mathrm{M}_2(\mathbb{Z}_{\ell^e})$, by which we mean that $\mathcal{A}$ equals its own centralizer, i.e., there is no matrix in $\mathrm{M}_2(\mathbb{Z}_{\ell^e}) \setminus \mathcal{A}$ that commutes with every element of $\mathcal{A}$. As an additive group, $\mathcal{A}$ must be isomorphic to

$$\mathbb{Z}_{\ell^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{\ell^{e_r}}, \qquad 2 \leq r \leq 4$$

for certain exponents $e = e_1 \geq \ldots \geq e_r$, just because

- it concerns a subgroup of $\mathrm{M}_2(\mathbb{Z}_{\ell^e}) \cong (\mathbb{Z}_{\ell^e})^4$,
- it contains $\mathbf{I}_2$, which has additive order ℓ^e,
- it contains at least one non-scalar matrix.

The following useful lemma implies that if $e_2 = e$, then necessarily $r = 2$ and as a result $\mathcal{A}$ is free when viewed as a $\mathbb{Z}_{\ell^e}$-module. We can indeed apply the lemma, because it is easy to see that if a matrix $\mathbf{M} = (m_{ij})$ is $\mathbb{Z}_{\ell^e}$-linearly independent of $\mathbf{I}_2$, then at least one of $m_{12}, m_{21}, m_{11} - m_{22}$ is a unit.

Lemma 11. *Let* $\mathbf{M} = (m_{ij}) \in \mathrm{M}_2(\mathbb{Z}_{\ell^e})$ *be such that* $\{m_{12}, m_{21}, m_{11} - m_{22}\}$ *contains a unit. Then the centralizer*

$$C_{\mathrm{M}_2(\mathbb{Z}_{\ell^e})}(\mathbf{M}) = \{\, \mathbf{X} \in \mathrm{M}_2(\mathbb{Z}_{\ell^e}) \mid \mathbf{MX} = \mathbf{XM} \,\},$$

when considered as a $\mathbb{Z}_{\ell^e}$*-module, is free of rank* 2.

Proof. Through the use of one of the conjugations

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} m_{22} & m_{21} \\ m_{12} & m_{11} \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} m_{11} - m_{12} & m_{12} \\ m_{11} - m_{12} + m_{21} - m_{22} & m_{12} + m_{22} \end{pmatrix}$$

we can reduce to the case where m_{21} is a unit. Expressing that a matrix $\mathbf{X} = (x_{ij})$ commutes with $\mathbf{M}$ leads to a system of equations

$$\begin{pmatrix} -m_{21}x_{12} + m_{12}x_{21} & -m_{12}x_{11} + (m_{11} - m_{22})x_{12} + m_{12}x_{22} \\ m_{21}x_{11} + (-m_{11} + m_{22})x_{21} - m_{21}x_{22} & m_{21}x_{12} - m_{12}x_{21} \end{pmatrix}$$
$$= \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} - \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

which can be checked to reduce to

$$\begin{cases} x_{11} = (m_{22} - m_{11})x_{21}/m_{21} + x_{22}, \\ x_{12} = m_{12}x_{21}/m_{21}. \end{cases}$$

From this the lemma follows. □

We call such a maximal commutative subalgebra *free*. Let us recall that this is a maximal commutative subalgebra $\mathcal{A} \subseteq \mathrm{M}_2(\mathbb{Z}_{\ell^e})$ whose additive group is isomorphic to

$$\mathbb{Z}_{\ell^e} \oplus \mathbb{Z}_{\ell^e},$$

and that this is automatically satisfied as soon as $\mathcal{A}$ admits an additive subgroup of this form.

Example 12. An example of a *non-free* maximal commutative subalgebra is the algebra of matrices of the form

$$\alpha \mathbf{I}_2 + \beta \ell \mathbf{M} \in \mathrm{M}_2(\mathbb{Z}_{\ell^2})$$

whose additive group structure is given by

$$\mathbb{Z}_{\ell^2} \oplus \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell.$$

Observe that its number of elements ℓ^5 is *larger* than $\ell^{2e} = \ell^4$ in this case!

Note that freeness comes for free if $e = 1$, i.e., when working over the field $\mathbb{F}_\ell$. In that case the following theorem is likely well-known.

Theorem 13. *Up to conjugation, the free maximal commutative subalgebras of* $\mathrm{M}_2(\mathbb{Z}_{\ell^e})$ *are given by*

$$\mathcal{A}_{c,d} = \{\, \mathbf{M}_{c,d}(ax + b) \mid a, b \in \mathbb{Z}_{\ell^e} \,\}$$

with $c, d \in \mathbb{Z}_{\ell^e}$. *Here* $\mathbf{M}_{c,d}(ax+b)$ *denotes the matrix of multiplication by* $ax+b$ *in the ring*

$$\frac{(\mathbb{Z}_{\ell^e})[x]}{(x^2 + cx + d)}$$

with respect to the basis $1, x$. *Moreover, writing* $\Delta_{c,d} = c^2 - 4d$, *two such subalgebras are conjugate if and only if*

$$\Delta_{c,d} = u^2 \Delta_{c',d'}$$

for some $u \in \mathbb{Z}_{\ell^e}^\times$.

Proof. It is easy to see that the algebras $\mathcal{A}_{c,d}$ are maximal commutative and free. Indeed, it is immediate that they are commutative and that their additive group structure is isomorphic to $\mathbb{Z}_{\ell^e} \oplus \mathbb{Z}_{\ell^e}$ (one can choose $\mathbf{I}_2 = \mathbf{M}_{c,d}(1)$ and $\mathbf{M}_{c,d}(x)$ as generators). Maximality then follows from the foregoing discussion.

To prove that every free maximal commutative subalgebra $\mathcal{A} \subseteq \mathrm{M}_2(\mathbb{Z}_{\ell^e})$ is conjugate to an algebra of the form $\mathcal{A}_{c,d}$, it suffices to show:

Claim. Every matrix in $\mathrm{M}_2(\mathbb{Z}_{\ell^e})$ is conjugate to a matrix

$$\mathbf{M} \in \mathcal{A}_{c,d}$$

for some $c, d \in \mathbb{Z}_{\ell^e}$.

Indeed, recall that $\mathcal{A}$ is additively generated by $\mathbf{I}_2$ and some non-scalar matrix $\mathbf{M}$. By the claim, we can assume that $\mathbf{M} \in \mathcal{A}_{c,d}$ for certain c, d. Every matrix in $\mathcal{A}_{c,d}$ commutes with $\mathbf{M}$ and therefore it commutes with every matrix in $\mathcal{A}$. Hence it follows from the maximal commutativity of $\mathcal{A}$ that $\mathcal{A}_{c,d} \subseteq \mathcal{A}$. But since $\mathcal{A}_{c,d}$ is maximal commutative, equality must hold.

To prove the claim, we argue that every matrix in $\mathrm{M}_2(\mathbb{Z}_{\ell^e})$ is conjugate to a matrix $\mathbf{M} = (m_{ij})$ satisfying

$$\nu_\ell(m_{21}) \leq \nu_\ell(m_{12}), \qquad \nu_\ell(m_{21}) \leq \nu_\ell(m_{22} - m_{11}).$$

This follows from the conjugations that were used in the proof of Lemma 11. Using a conjugation of the first kind we can ensure that $\nu_\ell(m_{21}) \leq \nu_\ell(m_{12})$. Once this is established, a conjugation of the second kind ensures that $\nu_\ell(m_{21}) \leq \nu_\ell(m_{22} - m_{11})$, as wanted. Consequently, there exist c, d such that

$$\mathbf{M} = \begin{pmatrix} m_{11} & -m_{21}d \\ m_{21} & m_{11} - m_{21}c \end{pmatrix},$$

but this is nothing else than $\mathbf{M}_{c,d}(m_{21}x + m_{11})$. Therefore $\mathbf{M} \in \mathcal{A}_{c,d}$.

Next, assume that two multiplication algebras $\mathcal{A}_{c,d}$ and $\mathcal{A}_{c',d'}$ are conjugates of each other, i.e., $\mathcal{A}_{c',d'} = \mathbf{T}\mathcal{A}_{c,d}\mathbf{T}^{-1}$ for some $\mathbf{T} \in \mathrm{GL}_2(\mathbb{Z}_{\ell^e})$. Let $\mathbf{M}$ be any matrix which along with $\mathbf{I}_2$ additively generates $\mathcal{A}_{c,d}$; then necessarily $\mathbf{M} = \mathbf{M}_{c,d}(ax+b)$ for some unit a. We also have that $\mathbf{TMT}^{-1}$ is a generator of $\mathcal{A}_{c',d'}$ along with $\mathbf{I}_2$, hence it is of the form $\mathbf{M}_{c',d'}(a'x + b')$ for some unit a'. Now it is straightforward to check the identity

$$\mathrm{disc}(\mathrm{charpol}(\mathbf{M}_{c,d}(ax+b))) = a^2\Delta_{c,d},$$

but since $\mathbf{M}$ and $\mathbf{TMT}^{-1}$ have the same characteristic polynomial this also equals $a'^2\Delta_{c',d'}$. We conclude that $\Delta_{c,d} = u^2\Delta_{c',d'}$ with $u = a'/a$.

Conversely, assume that $\Delta_{c,d} = u^2\Delta_{c',d'}$ for some unit u. One then checks that

$$\varphi : \frac{(\mathbb{Z}_{\ell^e})[x]}{(x^2 + cx + d)} \to \frac{(\mathbb{Z}_{\ell^e})[x]}{(x^2 + c'x + d')} : x \mapsto ux + \frac{uc' - c}{2}$$

is an isomorphism of rings; this is also true for $\ell = 2$, where we note that our assumption $\Delta_{c,d} = u^2\Delta_{c',d'}$ implies that $uc' - c$ has positive valuation, so that division by 2 makes sense. Writing $\mathbf{T}$ for the matrix of φ with respect to the bases $\{1, x\}$ and $\{1, x\}$, it readily follows that

$$\mathbf{M}_{c',d'}(\varphi(ax+b)) = \mathbf{T}\mathbf{M}_{c,d}(ax+b)\mathbf{T}^{-1},$$

showing that the algebras $\mathcal{A}_{c,d}$ and $\mathcal{A}_{c',d'}$ are conjugates of each other. □

Extrapolating from the case $e = 1$, the following nomenclature is natural; see also [22, App. A5]:

- The *split Cartan case* corresponds to $\Delta_{c,d}$ being a square unit. This case is unique up to conjugation. Taking $c = -1, d = 0$, we see that $\mathbf{M}_{c,d}$ consists of matrices of the form
$$\begin{pmatrix} b & 0 \\ a & a+b \end{pmatrix},$$
where we note that
$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ a & a+b \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} b & 0 \\ 0 & a+b \end{pmatrix}$$
so, up to conjugation, the split Cartan case corresponds to the subalgebra of diagonal matrices.
- The *non-split Cartan cases* correspond to $\Delta_{c,d}$ being a non-square unit. Usually this case is also unique up to conjugation: this is true as soon as $\ell > 2$ or $b < 3$; e.g. if $\ell \equiv 3 \bmod 4$ then we can realize it as the subalgebra of anticirculant matrices
$$\begin{pmatrix} b & -a \\ a & b \end{pmatrix}.$$
by taking $c = 0$ and $d = 1$. If $\ell = 2$ and $b \geq 3$ then there are three non-split Cartan cases, corresponding to whether $\Delta_{c,d} \bmod 8$ is 3, 5, or 7.
- The *ramified Cartan cases* correspond to $\Delta_{c,d}$ being a non-unit. These can be classified according to the valuation $v = \nu_\ell(\Delta_{c,d})$ and the class of the unit
$$\Delta_{c,d}/\ell^v \in \frac{\mathbb{Z}_{\ell^{e-v}}^*}{\mathbb{Z}_{\ell^{e-v}}^{*2}},$$
for which there are
  - 1 option if $v = e$ — this is the *totally ramified case*, corresponding to matrices of the form
$$\begin{pmatrix} b & 0 \\ a & b \end{pmatrix}$$
(e.g., take $c = d = 0$), up to conjugation — or also if $\ell = 2$ and $v = e-1$,
  - 2 options if $\ell > 2$ and $v < e$ or if $\ell = 2$ and $v = e - 2$,
  - 4 options if $\ell = 2$ and $v < e - 2$.

Example 14. The subalgebra of circulant matrices
$$\begin{pmatrix} b & a \\ a & b \end{pmatrix},$$
which have also been proposed for use in FESTA [3, Footnote 3], is precisely $\mathcal{A}_{0,-1}$, with discriminant 4. If $\ell > 2$ then this is the split Cartan case, while if $\ell = 2$ we are *almost* in the split Cartan case (we have $v = 2$ and $\Delta_{0,-1}/2^2 = 1$).

Subgroups

We now proceed to the study of maximal commutative subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell^e\mathbb{Z})$. Of course, by a maximal commutative subgroup we mean a subgroup that is equal to its own centralizer, but now considered inside $\mathrm{GL}_2(\mathbb{Z}/\ell^e\mathbb{Z})$. Note that we have commutativity-preserving maps

$$\mathcal{A} \mapsto \mathcal{A} \cap \mathrm{GL}_2(\mathbb{Z}_{\ell^e}) \subseteq \mathrm{GL}_2(\mathbb{Z}_{\ell^e}), \qquad G \mapsto \langle G \rangle_{\mathbb{Z}_{\ell^e}} \subseteq \mathrm{M}_2(\mathbb{Z}_{\ell^e})$$

between the set of subalgebras of $\mathrm{M}_2(\mathbb{Z}_{\ell^e})$ and the set of subgroups of $\mathrm{GL}_2(\mathbb{Z}_{\ell^e})$. To see that $\mathcal{A} \cap \mathrm{GL}_2(\mathbb{Z}_{\ell^e})$ is indeed a subgroup, it suffices to observe that if $\mathbf{M} \in \mathcal{A}$ is invertible, then also $\mathbf{M}^{-1} = (\det \mathbf{M})^{-1}(\mathrm{tr}(\mathbf{M})\mathbf{I}_2 - \mathbf{M}) \in \mathcal{A}$ by Cayley–Hamilton.

Lemma 15. *Every maximal commutative subgroup of* $\mathrm{GL}_2(\mathbb{Z}_{\ell^e})$ *is of the form* $\mathcal{A} \cap \mathrm{GL}_2(\mathbb{Z}_{\ell^e})$ *with* $\mathcal{A}$ *a maximal commutative subalgebra of* $\mathrm{M}_2(\mathbb{Z}_{\ell^e})$.

Proof. Let $G \subseteq \mathrm{GL}_2(\mathbb{Z}_{\ell^e})$ be a maximal commutative subgroup. Since $\langle G \rangle_{\mathbb{Z}_{\ell^e}}$ is commutative, we have that G is contained in a maximal commutative algebra $\mathcal{A}$. But then $G \subseteq \mathcal{A} \cap \mathrm{GL}_2(\mathbb{Z}_{\ell^e})$ and by the maximality of G, equality holds. □

The converse to this statement is slightly more subtle. But here is a special case where things work out:

Lemma 16. *If* $\ell > 2$ *then for any free maximal commutative subalgebra* $\mathcal{A} \subseteq \mathrm{M}_2(\mathbb{Z}_{\ell^e})$ *we have that* $\mathcal{A} \cap \mathrm{GL}_2(\mathbb{Z}_{\ell^e})$ *is a maximal commutative subgroup of* $\mathrm{GL}_2(\mathbb{Z}_{\ell^e})$.

Proof. Recall that $\mathcal{A}$ is additively generated by $\mathbf{I}_2$ and another matrix $\mathbf{M}$. We claim that $\mathbf{M}$ can be chosen to be an invertible matrix. To this end, consider

$$\det(\mathbf{M} + x\mathbf{I}_2) \bmod \ell \ \in \ \mathbb{F}_\ell[x]. \tag{9}$$

This polynomial has at most two roots, so since $\ell > 2$ we can find $\lambda \in \mathbb{Z}_{\ell^e}$ which does not reduce to a root of (9) modulo ℓ. If we then replace $\mathbf{M}$ with $\mathbf{M} + \lambda\mathbf{I}_2$ we find a generator that is invertible, as wanted.

Now the proof is easy. Let $\mathbf{N} \in \mathrm{GL}_2(\mathbb{Z}_{\ell^e})$ be a matrix that commutes with every matrix in $\mathcal{A} \cap \mathrm{GL}_2(\mathbb{Z}_{\ell^e})$. Then it commutes with $\mathbf{M}$, and therefore it commutes with every matrix in $\mathcal{A}$. From the maximality of $\mathcal{A}$ it follows that $\mathbf{N} \in \mathcal{A}$. □

In the foregoing lemma the condition $\ell > 2$ is necessary. Indeed, an easy counterexample is the split Cartan subalgebra

$$\mathcal{A} = \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\},$$

which is generated by

$$\mathbf{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad \mathbf{M} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Note that none of the matrices $\mu\mathbf{M} + \lambda\mathbf{I}_2$ with μ odd is invertible. Therefore $\mathcal{A} \cap \mathrm{GL}_2(\mathbb{Z}_{2^e})$ is contained in the index-2 subalgebra $\langle 2\mathbf{M}, \mathbf{I}_2 \rangle$. Every matrix in this subalgebra commutes with the invertible matrix

$$\begin{pmatrix} 1 & 2^{e-1} \\ 0 & 1 \end{pmatrix}$$

which is not contained in $\mathcal{A}$. Therefore $\mathcal{A} \cap \mathrm{GL}_2(\mathbb{Z}_{\ell^e})$ is not maximal commutative.

Remark 17. We end by remarking that with $\mathcal{A} \subseteq \mathrm{M}_2(\mathbb{Z}_{\ell^2}\mathbb{Z})$ the non-free maximal commutative subalgebra from Example 12, the resulting commutative subgroup $\mathcal{A} \cap \mathrm{GL}_2(\mathbb{Z}_{\ell^2})$ still contains $\ell^4(\ell-1)$ matrices, which is strictly larger than ℓ^4 as soon as $\ell > 2$. So this is still larger than what could be attained using free maximal commutative subalgebras.